Billing Code – 4910-HY

DEPARTMENT OF TRANSPORTATION

Enabling a Secure Environment for Vehicle-to-Vehicle and Vehicle-to-Infrastructure Transactions Workshop; Notice of Public Meeting

AGENCY: Research and Innovative Technology Administration, U.S. Department of Transportation

ACTION: Notice

The U.S. Department of Transportation (USDOT) Intelligent Transportation System Joint Program Office (ITS JPO) will hold a free Policy Research Workshop on Enabling a Secure Environment for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Transactions on April 19-20, 2012, 8:30 am – 5:00 pm at the Capital Hilton, 1001 16th Street, NW Washington DC, 20036, 202-393-1000. This two-day workshop will give participants an opportunity to learn about and provide input into research being conducted on potential organizational and business models for supporting security and data transaction needs for V2V and V2I crash avoidance and other applications. The workshop takes place mid-point for two related research efforts and will be structured primarily around breakout sessions for discussing critical issues and obtaining participant feedback. Final results of this research will be presented in August 2012 during the annual Connected Vehicle Safety public meeting and via other publicly available forums and on the ITS JPO website.

Persons planning to attend the workshop should register online no later than April 13, 2012 at *http://www.itsa.org/policyworkshop*. For additional questions, please contact Adam Hopps at Ahopps@ITSA.org.

About the Connected Vehicle Secure Environment

Establishing a secure trust environment among vehicles and other legitimate equipment is a key challenge for V2V and V2I crash avoidance and other applications. Currently a public key infrastructure approach to security involving the exchange of digital certificates among legitimate trusted vehicles and/or equipment is being analyzed and tested. USDOT's Connected Vehicle Policy Research Program is concerned with defining requirements to implement such a system on a national scale, including such questions as:

- What are the functional requirements for certificate exchange and other processes?
- What communications links and networks could support these requirements?
- What are the organizational requirements for supporting back end processes?
- What are estimated costs for supporting these requirements?
- What are potential business models for supporting such a network, to attract users and revenue to finance such a system?
- What do different approaches imply, in terms of potential levels of security protection?
- What do different ownership options imply?
- How could the certificate management system be rolled out across the nation over time?
- Are there opportunities to integrate needed functions into existing systems or organizations?

Issued in Washington, DC, on the 22th day of February 2012.

John Augustine,
Managing Director, ITS Joint Program Office

[FR Doc. 2012-4809 Filed 02/28/2012 at 8:45 am; Publication Date: 02/29/2012]